AMENDMENTS TO THE CLAIMS:

The listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method for securing the integrity of files prior to archiving of ~~said~~ the files, involving an exchange between a client and a Time Source Provider, ~~(a trusted third party) said~~ the method comprising the steps of:

the client generating a Public and a Private Key pair that is ~~organizationally~~ associated with an organization, a corporate unit or an individual;

the Time Source Provider generating a Ppublic and Pprivate Kkey pair for use in transactions with the client;

the client generating attributes of the ~~archived~~ files that are to be archived, the attributes includinges file sizes and cryptographic signatures;

encrypting the client's files with the client's Private Key and then with ~~utilizing~~ the ~~client's~~ Time Source Provider's Public Key ;

transmitting ~~said~~ the encrypted data and file attributes and the client's Public Key signature to ~~said~~ the Time Source Provider;

the Time Source Provider decrypting ~~said~~ the encrypted data and file attributes with the Time Source Provider's Private Key and then with the client's Public Key;

the Time Source Provider creating a Time Map containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client;

the Time Source Provider ~~returns~~ returning the client's data along with the time map and session key signature;

the Time Source Provider providing ~~said~~ the encrypted client data back to the client; and

the client ~~archives~~ archiving the original files, file attributes and the time map from ~~said~~ the Time Source Provider.

2. (Canceled)

3. (Original) A method as in claim 1, where the client provides multiple encryption of files, generating the signature of the file at each step, and providing all signatures along with the encryption key signatures to the Time Source Provider for inclusion of the time map.

4. (Canceled)

5. (Original) A method as in claim 1 for application of multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures.

6. (Currently Amended) A method as in claim 41, further comprising the steps of:

exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction;

the client producing ~~said~~ the archived files, file attributes and time map;

the Time Source Provider retrieving ~~said~~ the time map and session key;

the Time Source Provider regenerating ~~said~~ the time map;

the Time Source Provider encrypting ~~said~~ the time map with ~~said~~ the session key; and,

comparing ~~said~~ the regenerated time map to ~~said~~ the time map.

7. (Currently Amended) A method as in claim 1, further comprising the steps of:

establishing a clear channel transaction interval and pattern;

the client encrypting ~~said~~ the clear channel transaction using the client's Public and Private key pair;

sending ~~said~~ the clear channel transaction to the Time Source Provider;

triggering an alarm if ~~said~~ the clear channel transaction is not received by the Time Source Provider.

8. (New) A method as in claim 1, further comprising the steps of:

protecting the client's filenames via a filename lookup table having a signature;

transmitting the signature of the filename lookup table to the Time Source Provider.

9. (New) A method as in claim 1, further comprising the step of:

recording in the time map at least one of the time source, last synchronization to clock, location of the clock, last calibration of the clock, and the last time that the encryption keys for data exchange were updated.

10. (New) A method as in claim 9, further comprising the step of:

recording in the time map at least one of the list of archived files, the sizes of the archived files, and the signatures of any encrypted files.

11. (New) A method for securing the integrity of archived files for a client:

establishing a public and private key pair for the client, wherein the client's public and private key pair is associated with an organization, a corporate unit or one or more individuals;

generating a public and private key pair for use in transactions with the client;

receiving a data transmission from the client over a clear channel, wherein the data transmission includes encrypted data and archived file attributes and the client's Public Key signature and wherein the archived file attributes include data relating to the sizes of the files and cryptographic signatures and the archived files have been encrypted with the client's private key and with the time source provider's public key;

decrypting the encrypted data and file attributes with the time source provider's private key and then with the client's public key;

creating a time map containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client;

transmitting the encrypted client data along with the time map and session key signature over the clear channel to the client.

12. (New) The method as defined in claim 11, further comprising the steps of:

protecting the client's filenames via a filename lookup table having a signature;

transmitting the signature of the filename lookup table to the Time Source Provider.

13. (New) The method as defined in claim 12, further comprising the step of:

recording in the time map at least one of the time source, last synchronization to clock, location of the clock, last calibration of the clock, and the last time that the encryption keys for data exchange were updated.

14. (New) The method as defined in claim 13, further comprising the step of:

recording in the time map at least one of the list of archived files, the sizes of the archived files, and the signatures of any encrypted files.

15. (New) The method as defined in claim 14, further comprising the step of:

exchanging a session key between the client and the Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction;

retrieving the time map and session key;

regenerating the time map;

encrypting the time map with the session key; and,

comparing the regenerated time map the time map.

16. (New) The method defined in claim 15, further comprising the step of:

applying multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures.